# Mississippi Analysis & Information Center
## Social Media Policy

### Guidelines for the Use of Social Media by the MSAIC

Date: 03/05/2018

This Mississippi Analysis & Information Center *Social Media Policy* is applicable to all MSAIC operations and activities.

## I. PURPOSE

To establish guidelines for the use of social media in pre-employment background investigations, crime analysis and situational assessments, criminal intelligence development, and criminal investigations.

## II. POLICY

### A. GENERAL

Social media may be a valuable investigative tool to detect and prevent criminal activity. Data contained on the internet (including internet based mobile applications) within social networking sites may assist law enforcement in gathering timely information in furtherance of crime prevention, including the preservation of public order and the investigation of criminal activity, including suspected terrorist activity. Social media may also be used to make time sensitive notifications regarding special events, weather emergencies, or missing or endangered persons. While social media is a resource for law enforcement, employees must adhere to this policy to protect individuals' privacy, civil rights, and civil liberties and to prevent employee misconduct.

### B. LEGAL CONSIDERATIONS

MSAIC's use of social media will be conducted within the guidelines of 28 CFR Part 23. All MSAIC analysts will receive annual training regarding 28 CFR Part 23. All training provided by MSAIC Analysts pertaining to social media will include a section on civil rights and civil liberties. The proper use of social media requires the analyst to have a reasonable suspicion prior to gathering intelligence on a U.S. Citizen or Organization. Based on analysis of federal regulations, utilization of social media is a legal method of intelligence gathering for the following reasons:

1. There is no reasonable expectation of privacy on an Internet site not owned by the subject/organization.

2. The subject/organization has already released information to a third party in the form of the social media site.

3. Information posted to social media sites is publicly accessible and voluntarily generated. The opportunity not to provide information exists prior to the informational post by the user.

4. Individuals voluntarily post information on social media sites and have the ability to restrict access to posts as they see fit. Any information posted publicly can be used by the MSAIC in providing situational awareness and establishing a common operating picture.

## C. UTILIZATION OF SOCIAL MEDIA

The MSAIC will use internet based platforms that provide a variety of ways to follow activity related to monitoring publicly available online social media sites, forums, blogs, public websites, message boards and social gaming sites for information the MSAIC can use to provide situational awareness and establish a common operating picture. The MSAIC will gather, store, analyze and disseminate relevant and appropriate information to federal, state, local, and tribal law enforcement, and private sector partners authorized to receive such information. The MSAIC will use this information to fulfill a mission mandate to include the sharing of information with federal, state, local and tribal law enforcement and the private sector.

1. Social media may be used by MSAIC analysts for a valid law enforcement purpose. The following are valid law enforcement purposes:

    a. Pre-employment background investigations;

    b. Crime analysis and situational assessment reports;

    c. Criminal intelligence development; and

    d. Criminal investigations.

[redacted] MSAIC analysts will not:

    a. Actively seek personally identifiable information (PII) that is not connected to legitimate law enforcement purpose; or

    b. Post any information; or

    c. Actively seek to connect with other internal/external personal users; or

    d. Accept other internal/external personal users' invitations to connect; or

    e. Interact on social media sites.

3. Employees will only utilize social media to seek or retain information that:

    a. Is based upon a criminal predicate or threat to public safety; or

b. Is based upon reasonable suspicion that an identifiable individual, regardless of citizenship or U.S. residency status, or organization has committed an identifiable criminal offense or is involved in or is planning criminal conduct or activity that presents a threat to any individual, the community, or the nation and the information relevant to the criminal conduct or activity (criminal intelligence information); or

c. Is relevant to the investigation and prosecution of suspected criminal incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime; or

d. Is useful in crime analysis or situational assessment reports for the administration of criminal justice and public safety; or

e. Is relevant to pre-employment background investigations.

4. The MSAIC will not utilize social media to seek or retain information about:

a. Individuals or organizations solely on the basis of their religious, political, social views or non-criminal activities; or

b. An individual's participation in a particular non-criminal organization or lawful event; or

c. An individual's race, ethnicity, citizenship, place of origin, disability, gender, or sexual orientation unless such information is relevant to the individual's criminal conduct or activity or if required to identify the individual; or

d. An individual's age other than to determine if someone is a minor.

5. The MSAIC will not directly or indirectly receive, seek, accept, or retain information from:

a. An individual or nongovernmental information provider who may or may not receive a fee or benefit for providing the information if there is reason to believe that the information provider is legally prohibited from obtaining or disclosing the information; or

b. A source that used prohibited means to gather the information.

## D. AUTHORIZATION TO ACCESS SOCIAL MEDIA WEBSITES

This section addresses the authorization necessary to utilize social media and access social media websites for crime analysis and situational awareness/assessment reports; intelligence development; and criminal investigations.

1. Public Domain

    a. No authorization is necessary for general research, topical information or other law enforcement uses that do not require the acquisition of an online alias.

[redacted]

[redacted]

## E. AUTHORIZATION TO UTILIZE SOCIAL MEDIA TOOLS

Prior to utilizing a social media tool, the MSAIC Analyst will submit a request through the chain of command to the Deputy Director for authorization to use the social media tool. The social media tool may be utilized in criminal investigations; criminal intelligence development; and crime analysis and situational assessment reports (e.g. during sporting events, demonstrations or other large gatherings that require a law enforcement presence to ensure the safety of the public). The request must contain the following:

1. a description of the social media tool (s);

2. its purpose and intended use;

3. the social media websites the tool will access; and

4. the agency for which the request is being conducted.

The request must be reviewed by the MSAIC Privacy Officer prior to approval. In exigent circumstances, the MSAIC Analyst may utilize the social media tool and the requesting agency will provide a written request as soon as practical. The written documentation should include a description of the exigent circumstances and the verbal authorization, as well as the required information for the request.

## F. DOCUMENTATION AND RETENTION

Other than crime analysis and situational assessment reports, all information obtained from social media websites shall be placed within a case file, suspicious activity report, or intelligence report. At no time should MSAIC personnel maintain any social media files outside of these authorized files.

Crime analysis, situational assessment reports and threat assessments may be prepared for special events management, including First Amendment-protected activities. At the conclusion of the situation requiring the report or First Amendment-protected event where

there was no criminal activity related to the information gathered, the information obtained from the social media monitoring tool will be retained for no more than fourteen (14) days. Information from the social media monitoring tool that does indicate a criminal nexus will be retained in an intelligence report, suspicious activity report, or case investigative file as directed by the MSAIC retention schedule.

Information identified as criminal in nature that is obtained in the course of an investigation from a social media site will be collected and retained using screen shots, printouts of chat logs, copying uniform resource locators (URL's) for subpoena or investigatory purposes, or storing the information via secure digital means. When possible, employees will utilize investigative computer systems and software intended to record data from social media sites.

[redacted]

## H. DISSEMINATION

Retention and dissemination of social media information will be the same as the type of file, whether a paper or electronic file, in which the information is located. For example, retention and dissemination of social media information within an intelligence file will be treated in the same manner as an intelligence file. Information developed during the course of a criminal investigation will be provided to the law enforcement officer requesting the information and retained and disseminated in the same manner as the investigative case file.

## I. EMPLOYMENT BACKGROUND INVESTIGATIONS

As part of its employment background process, MSAIC personnel will conduct a search of social media websites and profiles in the public domain regarding the applicant. Applicants should not disclose passwords to social media sites or profiles to MSAIC personnel. In the event an applicant discloses their password, the MSAIC will not utilize the password to log into the applicant's social media site or profile. Agency Representatives/Intelligence Analysts will not search or attempt to gain access to private social media profiles. Investigations of an applicant's social media sites will be done using the following protocol:

1. All searches of applicant social media pages and profiles will only be for that information which is in the public domain.

[redacted]

3. Only criminal comments or images will be collected as part of the background investigatory process. Employees will not collect or maintain information about the political, religious, or social views, associations or activities of any individual or any group unless such information directly relates to criminal conduct or activity.

4. During the course of a background investigation, if a reference, supervisor, or colleague of the applicant provides negative information on the applicant related to a social media site, the MSAIC employee will prepare an investigative summary outlining the information provided by the reference.

## J. COMPLAINTS AND INFORMATION QUALITY ASSURANCE

1. Employees will report violations or suspected violations of this directive to the Privacy Officer in accordance with the MSAIC Privacy Policy.

2. Complaints from the public regarding information obtained from social media websites will be submitted to the Privacy Officer and handled in accordance with the MSAIC Privacy Policy. If the information is determined to be erroneous, the information will be corrected or deleted.

## K. PERSONAL SOCIAL MEDIA USE BY MSAIC EMPLOYEES

MSAIC Intelligence Analysts and representatives of MSAIC should exercise care if they choose to post personal information on the internet and use social media and social networking sites. MSAIC Intelligence Analysts and representatives should be mindful that social media communications become part of the worldwide electronic domain. Privacy settings and social media sites are subject to constant modifications and they should never assume that information posted on such sites is protected and secure. Firewalls and privacy claims by service providers cannot be trusted to safeguard information once it is posted on the internet. It should be expected that any information they create, transmit, download, exchange, or discuss in a public online forum may be accessed by the MSAIC without prior notice. Once information is posted, it is accessible by anyone and may result in unintended consequences, such as:

a. limiting future employment opportunities;

b. being viewed, altered, printed and redistributed by other internet users including criminal organizations;

c. jeopardizing the confidentiality and safety of themselves, family members, friends, and other Mississippi Analysis & Information Center employees.

The following social media activities are strictly prohibited by MSAIC Intelligence Analysts and their representatives:

a. Use of personal computers, cell phones or other internet devices to access internet sites which would have an adverse impact on the MSAIC or constitute a violation of the law.

b. Membership with, any organization or individual whose philosophies, creeds, policies, deeds or acts are in conflict with those of the MSAIC or law enforcement in general.

c. The publishing or posting of the department's logo, emblem, patch, letterhead or other official symbols unless authorized by the MSAIC Director.

d. Use of a real or alias personal social media account for posting, displaying or transmitting:

   1. Any communications that discredits or reflects poorly on the MSAIC, its missions or goals; or

   2. Any communication concerning MSAIC operations, personnel or MSAIC partner agencies; or

   3. Any official MSAIC business, whether oral or written; or

   4. Content that is disparaging to a person or group based on race, religion, sexual orientation, or any other protected class; or

   5. The nature of the employee's employment or work location; or

   6. MSAIC information to include, but not limited to: emails, records, documents, video recordings, audio recordings, or photographs to which the employee has access to as a result of employment; or

   7. Personal information concerning an employee or former employee of the MSAIC.

## L. SANCTIONS FOR MISUSE

Any MSAIC employees who are MDPS employee who violates the provisions of this directive will be subject to disciplinary action pursuant to MDPS policy, including termination. Other agency partner who are assigned to the MSAIC on a full or part-time basis who violate the provisions of this directive will be subject to removal from their assignment to the MSAIC and possible further disciplinary action by their respective agency.

**TERMS & DEFINITIONS:**

[redacted]

Crime Analysis and Situational Assessment Reports – Analytic activities to enable Mississippi Analysis & Information Center (MSAIC) to identify and understand trends, causes, and potential indicia of criminal activity, including terrorism.

Criminal Intelligence Information – Data which meets criminal intelligence collection criteria and which has been evaluated and determined to be relevant to the identification of criminal activity engaged in by individuals who or organizations which are reasonably suspected of involvement in criminal activity.

Criminal Nexus – Established when behavior or circumstances are related to an individual or organization's involvement or planned involvement in criminal activity or enterprise.

[redacted]

[redacted]

[redacted]

Public Domain –Any Internet resource that is open and available to anyone.

Social Media – A category of Internet-based resources that integrate user-generated content and user participation. This includes, but is not limited to, social media networking sites (Facebook, MySpace), micro blogging sites (Twitter), photo- and video-sharing sites (Flickr, YouTube), wikis (Wikipedia), blogs, and news sites (Digg, Reddit).

Social Media Tool – A tool used to capture data and monitor social media sites by utilizing automated tools such as web crawlers and word search functions to make predictive analysis, develop trends, or collect information. Examples include Netbase, Twitterfall, Trackur, Tweetdeck, Tweetgrid, Socialmention, Socialpointer, and Plancast. For this policy, reference to a "monitoring tool" refers to online tools that may be used continuously, within a specified time frame, to monitor social media activity related to an event or criminal and/or emergency situation where intelligence gathered from social media would facilitate in law enforcement situational awareness.

Social Networking – Utilization of web-based internet applications, including internet based mobile applications, which allow an individual to create an identity using his/her name or an alias.

Social Media Websites – Sites which focus on building online communities of people who share interests and activities and/or exploring the interests and activities of others. Social media websites are further categorized by Internet-based resources that integrate user-generated content and user participation. This includes, but is not limited to, social networking sites (Facebook, Myspace), micro blogging sites (Twitter, Nixle), photo-and video-sharing sites (Flickr, YouTube), wikis (Wikipedia), blogs, and news sites (Digg, Reddit). The absence of an explicit reference to a specific social media website does not limit the application of this policy.

Valid Law Enforcement Purpose – A purpose for information/intelligence gathering development, or collection, use, retention, or sharing that furthers the authorized functions and activities of a law enforcement agency, which may include the prevention of crime, ensuring the safety of the public, furthering officer safety, and homeland and national security, while adhering to law and agency policy designed to protect the privacy, civil rights, and civil liberties of Americans.